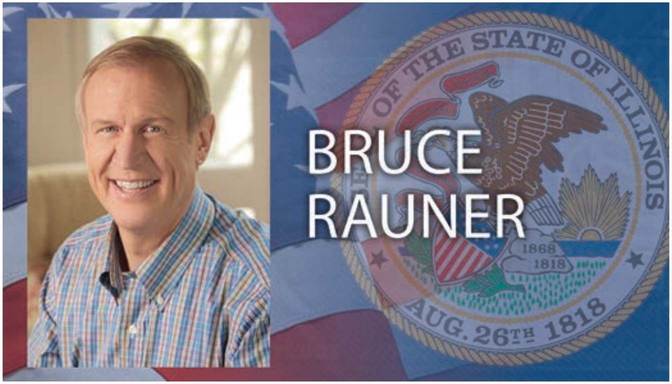
State of Illinois
Department of Innovation & Technology

State of Illinois Cybersecurity Strategy

2017 – 2019

Table of Contents

Goals and Objectives



Message from the Governor

Our vision for a more efficient, accessible, competitive and compassionate Illinois is being realized. The State of Illinois Digital Transformation is playing a key role by delivering best-in-class innovation and technology which is fostering collaboration, empowering state agencies to provide better services to our residents and maximizing the value of taxpayer resources.

Our expansion of the use of mobile technologies is providing ease in doing business with the state and enabling a more seamless engagement with our constituency. Illinois is unleashing the value of data resulting in rapid, more informed decision-making which is helping to protect our citizens. Illinois is leading the nation toward the development of a "Smart State" and hundreds of digital firms are launching in Illinois each year.

Our reliance on information systems continues to grow. Technology makes our world increasingly open with access to information in the palms of our hands. However, the services that we provide our citizens and the information we are entrusted with are increasingly at risk due to the cyber-threat.

Each day, cyber-criminals and other attackers attempt to gain access to our systems to disrupt state operations and steal the personal information of our citizens, employees and other constituents. States are increasingly targeted and these threats pose daily risks to Illinois' ability to serve its citizens and protect critical and confidential information. Due to these threats, I have prioritized cybersecurity as a key issue for my administration. As part of my Executive Order which created the Illinois Department of Innovation & Technology, I directed the Secretary to develop and implement policies and procedures to ensure the security of the state's information and systems. This strategy forms a solid foundation for the ongoing development and improvement of our cybersecurity capabilities and effectuates that protection.

The State of Illinois Cybersecurity Strategy has been developed in partnership with stakeholders across state government as well as other private and public sector stakeholders. The National Governors Association provided significant support as part of its Policy Academy for State Cybersecurity, which has facilitated collaboration across states as well as enabled vetting and finalization of the strategy.

The cybersecurity challenges we face are significant. However, I am convinced that through our collective dedication and hard work and with the support of our public and private sector partners, Illinois will continue to take significant steps toward establishing Illinois as one of the most cyber-secure states in the nation.

Governor Bruce Rauner Bruce Rauner

Message from the Chief Information Officer

Cybersecurity Goals Overview

I am pleased to issue the State of Illinois Cybersecurity Strategy for 2017 – 2019. This plan translates Governor Rauner's vision for a cyber-secure State of Illinois into an executable strategy which will help Illinois become one of the most cyber-secure states in the nation. This strategy focuses on five strategic goals:

- **Goal 1: Protect State of Illinois Information & Systems**
  Focuses on protecting the confidentiality, integrity, availability and cyber-resiliency of State of Illinois information and critical information systems to ensure the state's ability to deliver critical services to its citizens.

- **Goal 2: Reduce Cyber Risk**
  Creates the culture, frameworks and processes required to address cyber-risk, enhance decision making and better protect the state through continual risk awareness.

- **Goal 3: Best-in-Class Cybersecurity Capabilities**
  Develops the practices, processes, workforce and overall cybersecurity capabilities required to protect the state from the cyber-threat and ensure continual improvement to face tomorrow's cybersecurity challenges while ensuring the alignment of security priorities with the business needs and strategies of the state.

- **Goal 4: Enterprise Approach to Cybersecurity**
  Enhances cybersecurity across all agencies, boards and commissions that report to the Governor through the establishment of an enterprise-level cybersecurity program, and the adoption of best-practices, common frameworks, and enterprise information security policies. Most importantly, the State of Illinois technology transformation provides the unique opportunity to exponentially enhance the cybersecurity of state agencies.

- **Goal 5: A Cyber-Secure Illinois**
  Establishes the State of Illinois as a leader in cybersecurity across the state and the nation and enhances the cyber-security of the state as a whole through partnerships with both the public and private sector. The goal further provides enhanced protection to our citizens through the development of a comprehensive, statewide Cyber Disruption Plan, and provides a forward-leaning cybersecurity posture.

The State of Illinois Cybersecurity Strategy was developed through a comprehensive process which included an evaluation of current capabilities, cybersecurity maturity and risk assessments, input from leadership from state agencies, boards and commissions and evaluation of the current and evolving cyber threat landscape. The strategy development was enhanced through the active participation of the Governor's Technology Advisory Board and public and private sector partners.

Guidance and support from the National Governors Association (NGA) the National Association of State Chief Information Officers (NASCIO), the National Institute of Standards and Technology (NIST) and the community of state Chief Information Security Officers proved invaluable to this effort. Crucial strategic guidance was provided by the State of Illinois Executive Committee for Cybersecurity, which has helped ensure that cybersecurity is recognized not just as a business issue, but a matter of public safety concern.

Hardik Bhatt
State CIO, Secretary Designate
Department of Innovation & Technology

HBhatt

Threat Context

KIRK LONBOM
Chief Information Security Officer, State of Illinois

Chicago, Illinois skyline

The State of Illinois Cybersecurity Strategy is focused on reducing the risks to our citizens, ensuring the delivery of state services and protecting the state's critical infrastructure while enabling Illinois' digital transformation.

Millions of intrusion attempts are faced by the state on a daily basis. Attackers continually attempt to overwhelm the state's network to disrupt services. State employees face daily challenges as cyber-criminals pose as legitimate sources to gain trust, steal passwords and download malicious software. Criminals attempt to encrypt the state's data and hold it for ransom while nation-states attempt to steal personal information and even disrupt our democratic processes. Insider threats are of continual concern.

The challenges we face in protecting the privacy of our citizens, the confidentiality of our information and the ability to provide critical state services are vast. In addition, the State of Illinois must lead efforts toward a more cyber-secure state as a whole by helping to protect the state's critical infrastructure, prepare the state for potential cyber disruption, and promote cyber-security best-practices across the private and public sector.

Cyberattacks have been rising in both frequency and scale. The 2016 Global Risks Report, which examines the world-wide and regional impacts posed by threats such as the spread of infectious disease, the collapse of nation-states, food crises and weapons of mass destruction, identified that cyberattacks rank as the number one risk facing the United States. Terrorist attacks rank third.

As cyber-dependence rises, the resulting interconnectivity and interdependence can dilute the ability of organizations to sufficiently protect government and business operations. The growth of the Internet of Things, which will result in more connections between people and machines, will exponentially increase cyber-dependency, which will raise the likelihood of a cyber-attack having serious if not devastating cascading effects.[1]

- **Our Citizens** rely on life, health and safety services that are at risk from cyber-attack. The private information of our citizens must also be protected.
- **Critical Infrastructure** must be protected from life-threatening failure.
- **The Economy** is supported and growth is promoted through a cyber-secure Illinois.
- **Technology Vision** for the State of Illinois can only be realized by utilizing advanced technologies that are secure.
- **Risk** to life, health, safety and other critical services must be effectively managed.

Threat Context (cont.)

- **Our Citizens -** The State of Illinois provides countless services to improve the quality of life for our citizens. From state troopers to healthcare program personnel to child care case workers, there is strong reliance on the state's information systems to serve and protect the public. The State of Illinois delivers information from these systems via one of the largest state broadband networks in the nation, serving nearly 8,000 K-12 schools, libraries, museums, colleges and universities and local and state government. The cyber-threat poses ever-increasing risk to the state's ability to ensure consistent delivery of these services to its citizens.

  The State of Illinois is entrusted with the personal information of millions of its citizens and other constituents. Personally identifiable information, protected health information and information about children is held in State of Illinois systems and must be protected.

- **Critical Infrastructure** - Cyber-attacks against critical infrastructure are a reality. The cyber-threat to the state goes well beyond the risk of an information breach or an unavailable information system, but potentially impacts the lives of our citizens should critical infrastructure be impacted. The State of Illinois must play a leadership role in protecting the state's critical infrastructure from cyber-attack as well as preparing the state for the potential of life-threatening critical infrastructure failure.

- **The Economy** - The State of Illinois is the fifth-largest economy in the United States, with 34 Fortune 500 companies, 12 Global 500 companies and over one million small businesses. With all seven of the country's Class I Freight Railroads and the third largest interstate highway system, Illinois maintains a top seat in the national economy.

  Illinois is also a "State of Innovation." While State of Illinois governmental entities undergo an internal digital transformation, the state as a whole is driving innovation and technology growth by driving startup companies. In Chicago alone, over 275 digital firms launch each year.[2]

  An economically sound Illinois requires a cyber-secure Illinois. While risk-reduction results in cost avoidance, a cyber-secure Illinois supports business growth. A former cyber advisor to both the Bush and Obama Administrations stated: "Leaders must recognize that increased Internet connectivity can lead to economic growth, but only if that Internet connection and the devices connected to it are safe and secure. If countries, and states alike, do not invest equally in the security of the Internet, and the infrastructure that underpins it, the promise of economic growth will be transformed into a tax on growth."[3]

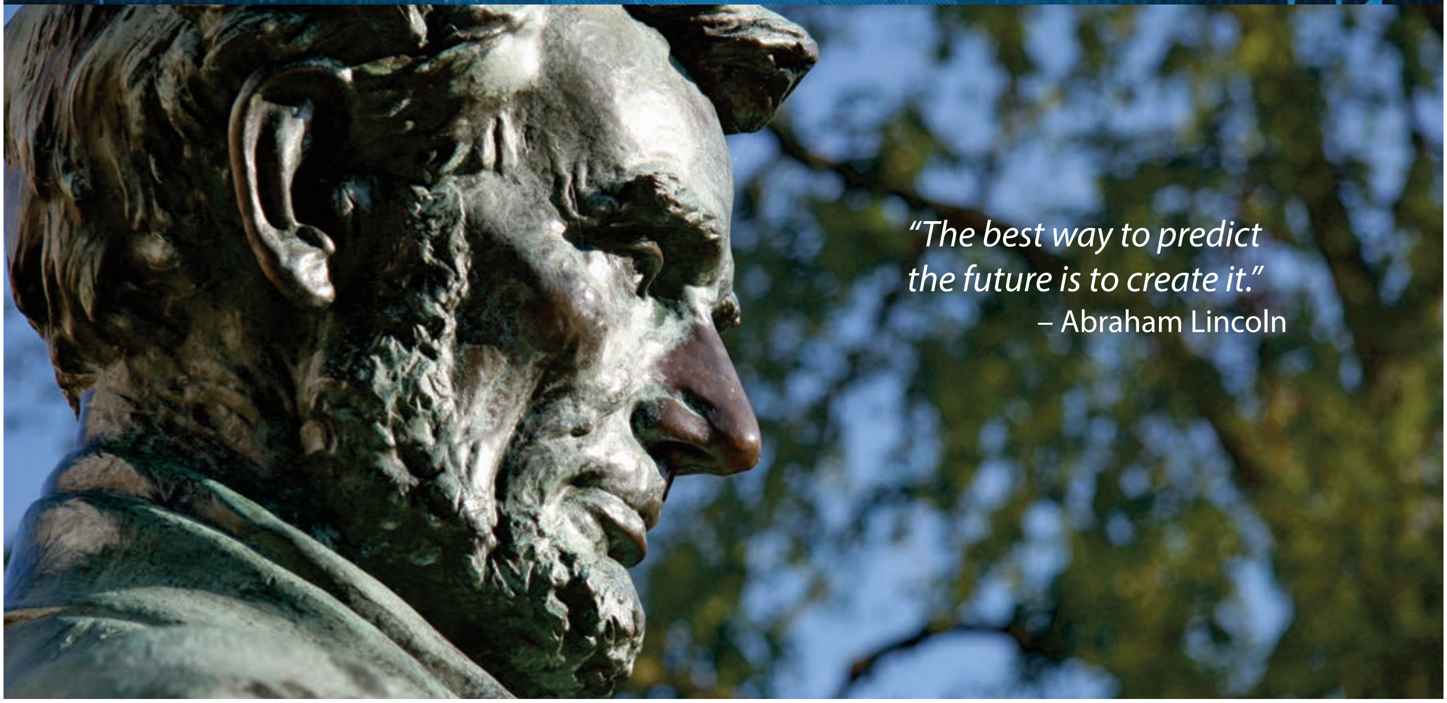
- **Technology Vision** - The State of Illinois is undergoing a digital transformation. The Illinois Department of Innovation & Technology is leading this transformation through an "Illinois First" strategy, which will address decades of technology neglect and catapult Illinois into a nationally recognized, advanced digital state. This vision includes establishing Illinois as a leader in the development of "A Smart State" and the use of cutting edge technologies.

  The neglect of information technology has also resulted in disparate and inconsistent information security practices which place the state at risk. As Illinois adopts cutting edge technologies, the cybersecurity function must keep pace. The State of Illinois Cybersecurity Strategy provides for establishing a modernized and forward-leaning cyber-security capability to both address current gaps as well as ensure the Illinois digital transformation can securely exploit modern technologies.

- **Risks** - The primary goal of information and cyber security programs is to reduce risk. Ensuring an understanding of 'what is at risk' has helped shape the cybersecurity strategy and will provide a foundation for cybersecurity program prioritization and resourcing. These risks are not just technology risks; rather they are life, health, safety and state business risks. The strategy was developed to reduce these risks.

> *"Leaders must recognize that increased Internet connectivity can lead to economic growth, but only if that Internet connection and the devices connected to it are safe and secure."*
>
> - Melissa Hathaway
>
> Former White House Cyber Advisor

Strategic Vision for Cybersecurity



"The best way to predict the future is to create it."
– Abraham Lincoln

Vision Statement - A secure and resilient cybersecurity environment which facilitates and protects the business of the State of Illinois, reduces risk and protects privacy, while promoting innovation, economic growth and transparency.

Strategic Guiding Principles

- Efforts to improve cybersecurity must properly reflect the borderless, interconnected, and global nature of today's cyber environment.
- Efforts to improve cybersecurity must be based on risk management.
- Efforts to improve cybersecurity must focus on awareness.
- Cybersecurity efforts must be able to adapt rapidly to emerging threats, technologies, and business models.
- Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.
- Efforts to improve cybersecurity must more directly focus on bad actors and their threats.
- Sufficient funding and resources must be provided to further the overall strategy.

The State of Illinois Cybersecurity Strategy provides an effective and focused roadmap for realizing Governor Rauner's vision for a Cyber Secure Illinois. The goals, objectives and action plans have been specifically developed and vetted to rapidly address any current gaps in cybersecurity operations while accelerating Illinois' progress toward the establishment of best-in-class cybersecurity capabilities. The comprehensive strategy maintains a laser focus on the Vision and a set of Strategic Guiding Principles which ensure a well-defined, deliberate and executable strategy.

The strategy ensures attention to the basic tenets and foundational information and cyber security concepts, processes and practices to protect the state while establishing a proactive approach to the advancing technological capabilities of the state. The State of Illinois digital transformation is placing Illinois in a leadership role across the nation in areas such as the exploitation of mobile technologies and data science. Illinois is also serving as the 'point of the spear' in the establishment of a 'Smart State' (utilizing the Internet of Things).[4] The State of Illinois Cybersecurity Strategy both builds foundational capabilities while being forward-leaning to support tomorrow's technology solutions.

Strategic Vision for Cybersecurity (cont.)

- **Strategic Roadmap** - While the cybersecurity strategy must identify action plans to enable the secure use of advancing technologies, the strategy must also provide a roadmap for ensuring the state can face the ever-growing and evolving cybersecurity threat landscape. The development of a robust cybersecurity organization, the consistent use of best-practices frameworks with measureable maturity levels and a focus on building an industry-aligned cybersecurity workforce are key components of the strategy to ensure the cyber-readiness of the state for years to come.

- **Focus on Risk** - The ever-growing reliance on technology solutions by state agencies, boards and commissions requires that cybersecurity programs align and support the business needs of the state. Our ability to deliver advanced and innovative technology capabilities which are secure is paramount to providing the high level of services that our citizens need and deserve. An effective and appropriate balance of nimble, innovative and secure solution delivery can be realized through sound cybersecurity risk management practices, secure solution engineering and effective cybersecurity governance, which are all critical components of this strategy.

- **From Defense to Resiliency** - Cyber-attacks are continuous and some will be successful. This realization exemplifies the importance that an effective cybersecurity strategy must include the development of robust cyber-defense and incident response and recovery capabilities. Proactive and deliberate cybersecurity monitoring and aggressive 'threat hunting' is required, as traditional network perimeter security alone can no longer protect the state from today's threat environment. The State of Illinois Cybersecurity Strategy includes significant focus on the critical areas of cyber-defense, threat intelligence, incident response and cyber-resiliency.

- **Securing the Enterprise** - A collective and enterprise-wide approach to cybersecurity is crucial to help protect the state from the impacts of cyberattacks. Historically, state agencies, boards and commissions have operated in cybersecurity silos, each with its own security policies, practices and protections. While some state agencies have maintained pace with the growing sophistication of attacks and increasing risk, most agencies lack the resources, expertise or focus to adequately protect their data and systems. The entire, interconnected State of Illinois network is placed at risk due to inconsistent, or sometimes, non-existent cybersecurity controls. This strategy addresses this critical issue through the establishment of a specific goal to ensure the State of Illinois addresses the cybersecurity challenge through an enterprise approach.

- **Leadership through Partnership** - Providing cybersecurity leadership across the state leads to a more cyber-secure Illinois across all sectors in the state. A key component to the vision of a cyber-secure Illinois includes a focus on public and private sector partnerships to help secure Illinois' critical infrastructure. The development of a comprehensive cyber disruption plan to help protect our citizens is a key deliverable of this strategy. Nurturing partnerships at all levels across government and private sector entities will provide leadership and facilitate continuous growth. Alignment with federal efforts ensures Illinois contributes to the overall improvement of the cybersecurity posture of the nation, but also provides key visibility to funding and joint cybersecurity initiatives which can benefit the state.

- **A "Grade A" Digital State** - Finally, a focus on executive involvement, effective communication and continual improvement provides the state with the ability to reduce cyber-risk as the State of Illinois becomes a "Grade A" digital state, positively impacting our services to our citizens, our security, and our economy.

Strategic Outcomes

State Capitol Building, Springfield, Illinois

The development of the State of Illinois Cybersecurity Strategy included an analysis of the current state of cybersecurity and the identification of the desired end-state. The cybersecurity goals, objectives and action plans were developed with a continuous eye toward the desired end-state characteristics. These characteristics have been translated into specific strategic outcomes.

The table below provides an alignment of the Cybersecurity Strategic Goals with these Targeted Outcomes.

TARGETED OUTCOMES FOR CYBERSECURITY STRATEGIC GOALS

Strategic Goal	Outcome
Goal 1 Protect State of Illinois Information and Systems	• State of Illinois information is protected from unauthorized disclosure. • State of Illinois information is trustworthy. • State of Illinois data and systems are available when needed. • The State of Illinois has the ability to withstand and quickly recover from deliberate attacks, accidents or naturally occurring threats or incidents. • A secure technology infrastructure helps protect the state from cyber-attack.
Goal 2 Reduce Cyber Risk	• Cybersecurity programs and initiatives are developed based on a sound and consistent risk management process across all state agencies. • A culture of cyber-risk awareness at all levels of government has been created and is continually enhanced. • Cybersecurity risk is clearly communicated understood, and owned by business executives.

Strategic Outcomes (cont.)

TARGETED OUTCOMES FOR CYBERSECURITY STRATEGIC GOALS (cont.)

Strategic Goal	Outcome
Goal 3 Best-In-Class Cybersecurity Capabilities	• Illinois cybersecurity strategies and programs are continually aligned with the business strategies of Illinois agencies, boards and commissions and the enterprise as whole. • Cyber-risk is reduced through the deployment of information systems that are secure. • The State of Illinois rapidly identifies and disrupts cyber-attacks to minimize adverse impact on the state. • Rapid, consistent and effective security incident response capabilities reduce the impact of security incidents, and response effectiveness is continually improved. • Illinois' cybersecurity workforce is well-trained, continually developed and aligned with national standards.
Goal 4 Enterprise Approach to Cybersecurity	• An effective enterprise-wide information and cybersecurity program provides for consistent cybersecurity protection across state agencies. • The cybersecurity posture of the state continues to improve through the use of a common cybersecurity framework. • Effective and consistent enterprise-wide cybersecurity policies are effectively communicated, monitored for compliance and resulting in a more secure enterprise. • The Illinois technology transformation and consolidation has resulted in a more cyber-secure state.
Goal 5 A Cyber Secure Illinois	• Illinois has established, exercised and continually improves an effective and inclusive cyber disruption strategy which will help reduce the impact of a cyber disruption on the state and its citizens. • The State of Illinois is leading efforts to improve the security of Illinois' critical infrastructure and protect Illinois citizens from cybercrime. • Illinois has developed and nurtured partnerships which foster continual learning and collaboration and effectively improves the state's cybersecurity posture. • Illinois contributes to the overall cybersecurity of the nation and utilizes national best-practices and frameworks. • The state is proactively identifying and utilizing alternative funding sources to improve the state's cybersecurity.

Goal 1: Protect State of Illinois Information and Systems

Abraham Lincoln Presidential Library and Museum - Springfield, Illinois

Protect the confidentiality, integrity, availability and cyber-resiliency of State of Illinois information and critical information systems to ensure the state's ability to deliver critical services to its citizens.

Goal 1 concentrates on the foundational information security objectives of ensuring the confidentiality, integrity and availability of critical information and systems. The premise that attacks will happen and some will be successful accentuates the need to create and maintain cyber-resiliency, which is the ability to anticipate, withstand, recover and evolve from adversary attacks. This goal helps ensure that State of Illinois information and systems are both resistant and resilient.

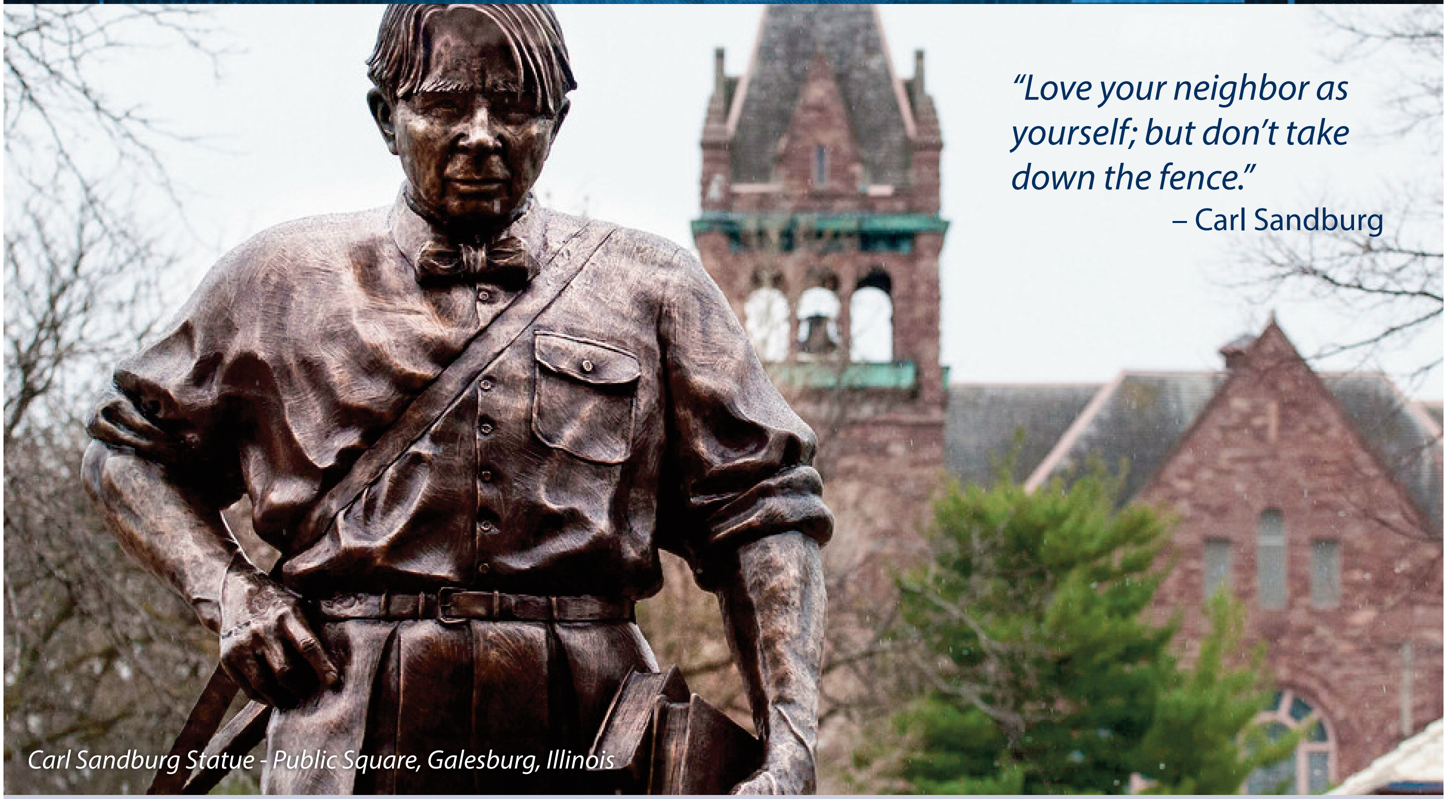
Under this goal, the State of Illinois will utilize disciplined and formal processes to identify and classify the state's most critical as well as confidential information and digital assets and apply the most cost-effective security controls commensurate with those findings. Absent this important discipline, adequate protections will not be identified, placing the state at increased risk. These processes further prevent ad hoc security investments, resulting in waste and a poorly protected state. Proactive monitoring requirements for critical systems will also be identified and implemented, enabling the state to quickly focus on threats against its most crucial assets.

The objectives which support this goal further include establishing the processes and technologies to verify the validity of data and protect it from being inappropriately altered. Information and system availability will be provided based on the needs of the state and the criticality of the services provided. Significant action will also be taken to harden the state's systems to be more resistant to cyber-attacks and rapidly identify and remediate security vulnerabilities. Executable recovery plans will be established to minimize the impact to state operations should a system fail due to attack or other event.

GOAL 1: PROTECT STATE OF ILLINOIS INFORMATION AND SYSTEMS

Objective	Action Plans
Objective 1.1 Safeguard Confidential Information from Compromise	• Identify confidential information through a formal data classification process. • Establish security controls to protect information in line with confidentiality requirements, laws and regulations. • Proactively monitor the systems which contain confidential information. • Ensure timely reporting of real or suspected information breaches and effectively manage information breach incidents. • Establish and maintain a "Zero Trust" model for network security.
Objective 1.2 Protect the Integrity of State of Illinois Information	• Develop and improve identity and access management capabilities commensurate with risk and integrity requirements. • Establish robust controls for securing and monitoring user accounts which have elevated privileges. • Deploy and enhance end-point protection and intrusion detection and prevention technologies commensurate with the growing threat landscape. • Expand the use of the State of Illinois Public Key Infrastructure to enhance data integrity, non-repudiation and authenticity. • Ensure data backup processes meet business requirements.
Objective 1.3 Ensure the Availability of Critical Information and Systems	• Obtain full understanding of critical system and information availability requirements based on agency priorities and mandates. • Identify and classify all technology assets which support critical information systems. • Ensure available protections and controls are in place for all technology assets commensurate with their value in support of critical information systems. • Confirm availability protections meet business requirements through periodic testing and validation.
Objective 1.4 Provide Cyber-Resilient Information Systems	• Develop business continuity and disaster recovery capabilities in line with State of Illinois business priorities. • Conduct system hardening on priority systems to provide the ability to withstand cyber-attacks. • Assist state agencies with identifying the most critical business processes and the development of information system contingency plans. • Determine the appropriate use of cybersecurity insurance to reduce cybersecurity incident impacts.
Objective 1.5 Maintain a Secure Technology Infrastructure	• Establish, maintain and monitor secure configurations for technology infrastructure. • Ensure effective vulnerability identification, prioritization and response. • Establish and maintain robust network monitoring and awareness capabilities. • Ensure cloud resources are securely deployed and remain secure. • Establish and maintain a Security Technology Lifecycle Plan.

Goal 2: Reduce Cyber Risk



> *"Love your neighbor as yourself; but don't take down the fence."*
> – Carl Sandburg

Carl Sandburg Statue - Public Square, Galesburg, Illinois

Create the culture, frameworks and processes required to address cyber-risk, enhance decision making and better protect the state through continual risk awareness.

Goal 2 addresses the overall goal of information and cyber security programs which is to protect the enterprise by reducing information and cyber security risk to an acceptable level. The changing face of technology as well as the growing cyber-threat requires a proactive approach to risk identification, prioritization and remediation. In addition, the State must create a culture of cyber-risk awareness at all levels of government, from state employees to constitutional officers. Through this goal, the State of Illinois will ensure decisions and investments are made based on sound risk management. The creation of a culture of cyber risk awareness further serves as a force-multiplier in keeping the state cyber-secure.

Objectives and action plans to realize this goal help establish a mature and consistent Risk Management Framework to ensure the State of Illinois understands the cyber-risks to the missions, information, assets, individuals and reputation of state agencies and the state as whole. The framework will combine risk assessments, risk communication, business executive-level risk ownership and the development of risk mitigation strategies into a comprehensive program which involves all levels of state government.

Creating a culture of cyber-risk awareness is key to the achievement of this goal. While annual cybersecurity awareness training is a component of the strategy, cybersecurity awareness must be continually developed and reinforced. Social engineering prevention programs and high-value target education are important components of this strategy.

GOAL 2: Reduce Cyber Risk	
Objective	**Action Plans**
Objective 2.1 Drive Cyber Security Priorities and Initiatives Based on Effective Risk Management	• Establish and mature an effective Risk Management Framework. • Conduct strategic risk assessments. • Develop risk mitigation strategies.
Objective 2.2 Create and Nurture a Culture of Cyber-Risk Awareness	• Create and maintain comprehensive information/cyber security awareness and privacy training programs. • Deliver social engineering prevention and detection programs. • Protect high-value personnel targets.
Objective 2.3 Establish Risk Ownership and Effectively Communicate Risk	• Establish cybersecurity risk governance at the agency, business vertical and enterprise levels. • Ensure cybersecurity risk acceptance is owned by state business executives. • Develop and execute cybersecurity risk communication plans.

Goals and Objectives

Goal 3: Best-in-Class Cybersecurity Capabilities

NCSA Petascale Computing Facility - University of Illinois , Champaign, Illinois

Create a best-in-class cybersecurity capability in line with best practices and national frameworks which facilitates and protects the business of the State of Illinois and contributes to the overall cybersecurity of the nation.

Goal 3 focuses on establishing and continually improving best-in-class cybersecurity practices, processes and workforce capabilities to ensure the state can effectively prepare, protect, defend, respond and recover in response to today's cyber-threat environment as well as prepare for tomorrow's cybersecurity challenges.

The State of Illinois provides myriad services to support its citizens, many of which help ensure life, health and safety. Significant resources are expended each and every day to deliver these services to help maintain and improve the quality of life for Illinois' citizens and visitors as well as provide a robust business environment critical for Illinois' economy. The growing reliance on information systems and other technology requires that Illinois establish and maintain the capabilities to protect the state from the threats posed by cyber-attacks which continue to increase both in volume and sophistication.

It is critical that cybersecurity functions and processes support the business needs of the state. This "business security alignment" priority is delivered through this goal while the state develops and continually improves best-in-class cybersecurity capabilities in the areas of security engineering, incident response and cyber-defense.

As the State of Illinois executes its digital transformation, the state is rapidly advancing the use of cloud, mobility and data technologies. Illinois is also leading the nation in the development of a "Smart State" utilizing Internet of Things technologies and researching the use of other technologies for tomorrow's solutions. This goal seeks to not only establish best-in-class capabilities for cybersecurity, but will strive for 'first-in-class' in these emerging areas.

GOAL 3: BEST-IN-CLASS CYBERSECURITY CAPABILITIES	
Objective	**Action Plans**
Objective 3.1 Ensure the Alignment of Information and Cyber Security Efforts with the Business Needs of the State	• Align cybersecurity programs and activities with the information technology priorities of the state enterprise and state agencies, boards and commissions. • Ensure the security and compliance requirements of state agencies are met. • Establish and maintain formal cybersecurity governance. • Facilitate executive communications and support.
Objective 3.2 Deliver Technology Solutions that are Secure	• Establish secure systems development and acquisitions processes and expertise. • Assure the security of third-party solutions. • Enable the secure optimization of mobile technologies. • Provide secure cloud utilization. • Facilitate the secure use of big data. • Ensure a secure "Smart Illinois".
Objective 3.3 Enhance the State's Ability to Detect Cyber-Attacks	• Establish a best-in-class Security Operations Center (SOC). • Establish and continually improve robust cyber-attack detection capabilities. • Continually identify indicators of compromise.
Objective 3.4 Respond Rapidly and Effectively to Security Incidents	• Establish and continually improve the State of Illinois Security Incident Response Program. • Establish clear and mandatory security incident reporting policies and procedures. • Exploit automation for security incident identification and management.
Objective 3.5 Build and Maintain a Robust Cyber-Defense Capability	• Detect and prevent threats at every point across the attack lifecycle. • Optimize the use of cyber-threat intelligence. • Deploy advanced cyber-defense processes and technologies. • Establish cyber-threat hunting capabilities.
Objective 3.6 Develop and Sustain a Capable and Competent State of Illinois Cybersecurity Workforce	• Build a robust State of Illinois cybersecurity organization. • Provide the State of Illinois cybersecurity workforce with career growth and advancement opportunities. • Recruit and hire highly skilled talent. • Provide effective training and assist employees in obtaining applicable information security certifications. • Provide for the development and recruitment of the next generation cybersecurity workforce. • Promote continual learning through partnerships.

Goal 4: Enterprise Approach to Cybersecurity

Chicago, Illinois skyline

Enhance the cybersecurity of the state through an enterprise, standards-based approach and the adoption of best-practices, common frameworks and enterprise information security policies and programs.

Goal 4 will enhance the cybersecurity posture of the state through the establishment of an enterprise-wide cybersecurity program. Disparate and inconsistent cybersecurity practices across state agencies, boards and commissions which place the state at increased risk will be replaced by enterprise security policies and standards, consistent, effective and protective technologies and formal information security processes based on best-practices.

The program will be driven by enterprise information and cyber security policies, standards, procedures and guidelines. Through an enterprise approach, executive support and management commitment to cybersecurity will be clearly established. Information security standards based on guidance from the National Institute of Standards and Technology, federal regulations and best-practices will ensure security policy implementations and operations both protect the state and ensure regulatory compliance.

The NIST Cybersecurity Framework is rapidly becoming the national standard across both the public and private sectors. The State of Illinois has adopted the NIST Cybersecurity Framework for the development and improvement of Illinois' cybersecurity program. Embracing this framework across the State of Illinois enables the state to better understand, manage and reduce cybersecurity risk, enhances communication through the establishment of a common language and provides a consistent cybersecurity maturity measurement capability. While flexible, the adoption of the NIST Cybersecurity Framework as part of the enterprise approach to cybersecurity provides all agencies, boards and commissions with a common and widely-accepted roadmap.

The overall cybersecurity of the State of Illinois will be greatly enhanced through the state's technology transformation. The establishment of the Department of Innovation & Technology as the state's centralized information technology organization further facilitates the adoption of common security practices. Through infrastructure consolidation, the state can more effectively provide enterprise-class cybersecurity protections and controls, resulting in a more secure state.

GOAL 4: ENTERPRISE APPROACH TO CYBERSECURITY	
Objective	**Action Plans**
Objective 4.1 Establish the State of Illinois Information and Cyber Security Program	• Establish the State of Illinois Information and Cyber Security Program through issuance of formal policy. • Develop the State of Illinois Information and Cyber Security Program in line with NIST guidance and industry best-practices.
Objective 4.2 Embrace a Common Cybersecurity Framework	• Improve the State's cybersecurity maturity against the NIST Cybersecurity Framework. • Promote the use of the NIST Cybersecurity Framework across Illinois. • Help drive the national vision for the NIST Cybersecurity Framework.
Objective 4.3 Enact Effective Enterprise-Wide Security Policies	• Establish enterprise security policy governance. • Develop enterprise security policies based on national standards, federal regulations, best practices and the needs of the state. • Establish clearly-defined security standards, procedures and guidelines.
Objective 4.4 Improve State Agency Security through the State's Technology Transformation	• Conduct agency security and risk assessments. • Ensure understanding of agency business strategies and security requirements. • Enhance agency security compliance and audit response efficiency. • Enhance the cyber-resiliency of state agencies. • Fully integrate agencies into enterprise security policies, practices and services.

Goal 5: A Cyber Secure Illinois

Inside Capitol Dome - Springfield, Illinois

Create a Cyber Secure Illinois and contribute to the national vision for cybersecurity through leadership, partnership and national participation.

Goal 5 seeks to address the borderless, interconnected, and global nature of today's cyber environment by recognizing the critical need to work collectively across the state, and the nation, to help protect our citizens, our state and the national security. The State of Illinois has the opportunity to assume a leadership role to drive the overall cybersecurity of the state while contributing to, and learning from, our partners across all sectors.

A cornerstone to this goal is the development of a Statewide Cyber Disruption Strategy. The State of Illinois and the critical infrastructure within the state are at risk from cyber-attacks that could disrupt government operations and negatively impact our citizens. The development of the Statewide Cyber Disruption Strategy will bring together partners across both the public and private sector, the National Guard and mission-critical state agencies. This plan will be a key component of the Illinois Emergency Operations Plan, and overseen by the Illinois Emergency Management Agency. The development of this strategy will establish capabilities intended to eliminate or limit cyber events and the potential negative effects of such an event. [5]

Action plans which support this goal also focus on establishing and nurturing partnerships across the state. Through outreach and collaboration with other state and local governmental entities, best-practices can be shared to help guide those entities which lack expertise and resources while learning from more cyber-advanced organizations. Through partnerships, the State will also identify opportunities for collaboration as well as identify potential funding for cybersecurity initiatives.

Through active participation with federal partners, the State of Illinois will remain on the front lines of emerging programs and initiatives, developing standards and further help drive the national strategy. Aligning with the national vision also provides the potential for acquiring funding from federal initiatives. This goal further provides the action plans to be forward-leaning in the development of security practices which will enable the secure use of emerging technologies.

GOAL 5: A CYBER SECURE ILLINOIS

Objective	Action Plans
Objective 5.1 Improve the state's cybersecurity through leadership, partnerships, and national participation	• Develop and continually improve a Statewide Cyber Disruption Strategy. • Establish the Illinois Department of Innovation & Technology as a leader and key service provider to drive cybersecurity improvement efforts across the state. • Establish, maintain and nurture partnerships and effective communication with public and private sector partners to collectively defend the state from cyber-attacks. • Lead the nation in the development of cybersecurity practices which address emerging and expanding technologies. • Closely align Illinois' ongoing cybersecurity strategies with the national vision. • Maximize the use of cybersecurity funding opportunities.

Endnotes

1. "The Global Risk Report 2016." World Economic Forum, www.weforum.org/reports.the-global-risks-report-2016.

2. "Illinois: The State of Innovation." Business Climate, www.businessclimate.com/illinois-economic-development-digital-magazine/.

3. "State of the States On Cybersecurity." The Pell Center, 2015, www.pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.

4. "Illinois Seeks to Become the Nation's First Smart State." TechRepublic, www.techrepublic.com/article/illinois-seeks-to-become-the-nations-first-smart-state/.

5. "Cyber Disruption Response Planning Guide." NASCIO.org, www.nascio.org/Surveys/ArtMID/557/ArticleID/358/Cyber-Disruption-Response-Planning-Guide.

Appendix

Alignment With NIST Cybersecurity Framework

Alignment of the State of Illinois Cybersecurity Strategy with the NIST Cybersecurity Framework	Identify	Protect	Detect	Respond	Recover
Strategic Goal #1 - Protect State of Illinois Information and Systems					
Objective 1.1 - Safeguard Confidential Information from Compromise		▨			
Objective 1.2 - Protect the Integrity of State of Illinois Information		▨			
Objective 1.3 - Ensure the Availability of Critical Information and Systems		▨			
Objective 1.4 - Provide Cyber-Resilient Information Systems		▨		▨	▨
Objective 1.5 - Maintain a Secure Technology Infrastructure		▨			▨
Strategic Goal #2 - Reduce Cyber Risk					
Objective 2.1 - Drive Cybersecurity Priorities and Initiatives Based on Effective Risk Management	▨	▨	▨	▨	▨
Objective 2.2 - Create and Nurture a Culture of Cyber-Risk Awareness	▨	▨	▨		
Objective 2.3 - Establish Risk Ownership and Effectively Communicate Risk	▨				
Strategic Goal #3: Best-in-Class Cybersecurity Capabilities					
Objective 3.1 - Align Information and Cyber Security Efforts with the Business Needs of the State	▨	▨	▨	▨	▨
Objective 3.2 - Deliver Technology Solutions that are Secure		▨			
Objective 3.3 - Enhance the State's Ability to Detect Cyber-Attacks			▨		
Objective 3.4 - Respond Rapidly and Effectively to Security Incidents				▨	▨
Objective 3.5 - Build and Maintain a Robust Cyber-Defense Capability		▨	▨	▨	
Objective 3.6 - Develop and Sustain a Capable and Competent State of Illinois Cybersecurity Workforce	▨	▨	▨	▨	▨
Strategic Goal #4 - Enterprise Approach to Cybersecurity					
Objective 4.1 - Establish the State of Illinois Information and Cyber Security Program	▨	▨	▨	▨	▨
Objective 4.2 - Embrace a Common Cybersecurity Framework	▨	▨	▨	▨	▨
Objective 4.3 - Enact Effective Enterprise-Wide Security Policies	▨	▨	▨	▨	▨
Objective 4.4 - Improve State Agency Security through the State's Technology Transformation	▨	▨	▨	▨	▨
Strategic Goal #5 - A Cyber-Secure Illinois					
Objective 5.1- Improve the State's Cybersecurity through Leadership, Partnerships and National Participation	▨	▨	▨	▨	▨

Printed by Authority of the State of Illinois

IOCI 17-34